IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	CASE NO.: 1:16CR224
	)	
Plaintiff,	)	JUDGE PATRICIA A. GAUGHAN
	)	
v.	)	
	)	
BOGDAN NICOLESCU, et al.,	)	SENTENCING MEMORANDUM
	)	
Defendants.	)	

Now comes the United States of America, by its counsel, Michelle M. Baeppler, First Assistant United States Attorney, Duncan T. Brown and Brian M. McDonough, Assistant United States Attorneys, and hereby submits this Sentencing Memorandum, and respectfully requests this Court sentence defendants BOGDAN NICOLESCU and RADU MICLAUS to terms of incarceration of 240 months and 216 months respectively for the reasons argued below.

I. BACKGROUND HISTORY

On July 8, 2016, a nine-year FBI investigation culminated with a grand jury in the Northern District of Ohio returning a 21-count Indictment against BOGDAN NICOLESCU, TIBERIU DANET, and RADU MICLAUS, charging them with the offenses of Conspiracy to Commit Mail and Wire Fraud, Conspiracy to Obtain Unauthorized Access to a Protected Computer, Aggravated Identity Theft and Conspiracy to Commit Money Laundering. The government extradited the Defendants from Romania and they had their initial appearance before this court on December 20, 2016. On November 6, 2018, defendant DANET entered into a plea agreement in which he agreed to provide cooperation in return for a sentence of between nine and twelve years of incarceration.

The trial for NICOLESCU and MICLAUS commenced on March 25, 2019. In its case-in-chief the government called 28 witnesses[1] and introduced approximately 128 exhibits over approximately two-and-a-half weeks. Neither defendant presented a case; after about a day-and-a-half of deliberation, the jury returned a verdict of guilty for both NICOLESCU and MICLAUS on all 21 counts.[2]

On December 6, 2019, an extensive sentencing hearing was held during which testimony from SSA Ryan Macfarlane was taken, along with statements from multiple victims were presented. The transcript of that hearing is attached as Exhibit A hereto and incorporated and adopted for this memorandum. At the end of the hearing this Court sentenced NICOLESCU to concurrent imprisonment terms of 216 months on Counts 1 through 13 and 21; 60 months on Count 14; and 120 months on Count 15. (R. 198: Judgment, PageID 3062-63). The court also sentenced NICOLESCU to 24 months imprisonment on Counts 16 through 20 to run concurrently with each other, but consecutively to the other counts, for a total sentence of 240 months imprisonment. (Id., PageID 3063).

That same day, the court sentenced MICLUAS to concurrent imprisonment terms of 192 months on Counts 1 through 13 and 21; 60 months on Count 14; and 120 months on Count 15.

[1] Witnesses traveled from two continents, two foreign countries, and 11 different states.

[2] The jury did not find in favor of a sentencing enhancement under 18 U.S.C. § 3559(g) for falsely registering a domain name during commission of a crime. Liam O'Murchu from Symantec, however, testified that he saw all of the domain names listed in the Indictment used to communicate with Symantec's computers that were infected with the Bayrob Virus. Further, Supervisory Special Agent (SSA) Ryan Macfarlane testified that he found evidence on the Bayrob Group's command and control servers that each of these domains was falsely registered by the Bayrob Group. Further, in his plea agreement, DANET specifically admitted to intentionally registering all of the domains at issue using false identities. Dkt. 99-1 at ¶ 71. As discussed below, the Guidelines contemplate an upward enhancement of two levels for such conduct.

(R. 201: Judgment, PageID 3075-76). The court also sentenced MICLAUS to 24 months imprisonment on Counts 16 through 20 to run concurrently with each other, but consecutively to the other counts, for a total sentence of 216 months imprisonment. (Id., PageID 3076).

The defendants both appealed arguing several sentencing errors, and the government conceded error on the application of USSG 2B1.1(b)(19)(A)(ii), applying four levels for a conviction under 18 USC 1030(a)(5)(A). The Sixth Circuit also held that the application of 2 levels enhancement pursuant to USSG 2B1.1(b)(4) was not consistent with other courts, and, on November 9, 2021, remanded the case back to this court for resentencing consistent with their calculation of the defendants' adjusted sentencing range of an Adjusted Offense Level of 37, Criminal History I, 210 to 262 months, prior to the addition of any additional periods of incarceration required for their convictions of Aggravated Identity Theft, 18 U.S.C. §1028A. The Sixth Circuit, in its order of remand, noted that the adjusted Guideline range still encompasses the sentences both defendants received, but was not sure the five-level decrease from Level 43 to Level 38 in the original sentencing would still be applied to the new Adjusted Offense Level.

Simply, the government argues that the defendants should be sentenced using an Adjusted Offense Level of 37 and that the five-level departure granted at the original hearing is not appropriate on remand. The government argues that at the hearing it was clear the five-level departure was agreed to in order to bring the defendants into a sentencing range of the Guidelines table that contained 240 months, the statutory maximum, and thus a five-level departure is not necessary or appropriate because the range identified by the Sixth Circuit includes 240 months.

Indeed, based on the extensive evidence considered by the Court, and the appropriateness of the Court's application of the existing enhancements, sentences consistent with the

defendants' original sentences is appropriate. Specifically, NICOLESCU should receive a within-Adjusted Guidelines sentence of 216 months, and MICLAUS should receive a below-Adjusted Guidelines sentence of 192 months, and each receive a consecutive sentence of 24 months to each term, for a total of 240 months for NICOLESCU and 216 months for MICLAUS, with credit for any time served to this point.

II. STATUTORY SENTENCES

On remand, the defendants' convictions were AFFIRMED and thus, their statutory sentences remain the same.

The Defendants were charged in Count 1 with Conspiracy to Commit Wire Fraud, in violation of Title 18 U.S.C. §§ 1343 and 1349. The maximum term of imprisonment is 20 years, with a $250,000 maximum fine, three years of supervised release and a $100 special assessment due at time of sentencing.

The Defendants were charged in Counts 2-13 with Wire Fraud, in violation of Title 18 U.S.C. §1343. For each count of substantive Wire Fraud, the maximum term of imprisonment is 20 years, with a $250,000 maximum fine, three years of supervised release and a $100 special assessment due at time of sentencing.

Count 14 charged the Defendants with Conspiracy to Obtain Unauthorized Access to a Protected Computer in violation of 18 U.S.C. §§ 1030(a)(2)(c), 1030(a)(4), 1030(a)(5)(A) and (c)(4)(B), in violation of Title 18 U.S.C. § 371. The maximum term of imprisonment is 5 years, with a maximum fine of $250,000, three years of supervised release and a $100 special assessment due at time of sentencing.

Count 15 charged the Defendants with Conspiracy to Traffic in Counterfeit Service Marks in violation of Title 18 U.S.C. § 2320(a)(1). The maximum term of imprisonment is 10

years, with a maximum fine of $250,000, three years of supervised release and a $100 special assessment due at time of sentencing.

The Defendants were charged with five counts of Aggravated Identity Theft in Counts 16-20, in violation of 18 U.S.C. §1028(A). Each conviction carries a consecutive two-year prison sentence which run concurrent to each other and consecutive to the rest of the sentence. Each count also imposes a fine of up to $250,000, three years of supervised release and a $100 special assessment due at time of sentencing.

Count 21 charged the Defendants with Conspiracy to Commit Money Laundering, in violation of Title 18 U.S.C. §1956(h). The maximum term of imprisonment is 20 years, with a maximum fine of the greater of $500,000 or twice the value of the property involved in the transactions, three years of supervised release and a $100 special assessment due at time of sentencing.

III. RESENTENCING SHOULD BE BASED ON A LIMITED ORDER OF REMAND

It is well-settled that appellate courts have the authority to order general or limited remands under 28 U.S.C. § 2106. *United States v. Moore*, 131 F.3d 595, 597 (6th Cir. 1997); *accord United States v. McFalls*, 675 F.3d 599, 604 (6th Cir. 2012); *United States v. Campbell*, 168 F.3d 263, 265 (6th Cir. 1999). This Court has routinely addressed this rule in the context of remands for resentencing. *Campbell*, 168 F.3d at 265. While a general remand allows the district court to consider new evidence and issues at resentencing, a limited remand "constrains the district court's sentencing authority to the issue or issues remanded." *Id*. In fact, limited remands "explicitly outline the issues to be addressed by the district court and create a narrow framework within which the district court must operate." *Id*.

When not otherwise specified, there is a strong presumption that an appellate court's remand order is general. *McFalls*, 675 F.3d at 604. But when the appellate court's mandate is "so narrow in scope as to preclude the district court from considering a particular issue," the remand is limited and constrains the district court's authority significantly. *Id*. Appellate courts must use "unmistakable" language and "leave no doubt in the district judge's or parties' minds" to affect a limited remand. *Campbell*, 168 F.3d at 267.

A. The Sixth Circuit Ordered a Limited Remand

The government argues that the remand by the Sixth Circuit was a limited remand specifically tailored to the issue of whether or not, using a "correctly calculated range," the sentencing court would find the downward departure originally applied be appropriate. (R. 75-3: Sixth Circuit Remand, PageID 28). The order of remand was based on a lengthy quote from *United States v. Montgomery*, 998 F.3d 693, 700 (6th Cir. 2021), which addressed the propriety of downward departures on remand, and an exhaustive discussion of Guideline calculations based on the hearing transcript; the government argues that reading this remand using the plain and unmistakable language of the order requires a remand limited so "Nicolescu and Micluas can be resentenced under a correctly calculated Guidelines range." *Id*. at 28.

B. In the Alternative, the Government Requests a *De Novo* Resentencing and Argues Restitution be Imposed for Both Defendants

In the alternative, if the review is *de* novo, the government proffers into the record the transcript from the sentencing hearing held on December 6, 2019 as well as the Sixth Circuit's order of remand and incorporates its findings of fact underlying the calculation of Guideline enhancements consistent with the underlying findings of fact by the Sentencing Court. Based on that proffered evidence, the government argues that the defendants would face the same fate at sentencing. Under a *de novo* review, the government would seek a loss amount of 30 million

dollars, which would make their enhancement for loss to be **22,** not **18**, and thus, their Adjusted Base Offense level would be **41**. However, because the sentencing range must be inclusive of 240 months, the Court would have to grant a departure to an Adjusted Offense Level **38**, and their range would be 235 to 240 months, as it was at the original sentencing. Regardless of their Adjusted Base Offense level being **37** or **38**, the government requests sentences for both defendants consistent with their original sentences.

What the government does request pursuant to a *de novo* order of remand is restitution. The government requests that the Court find NICOLESCU and MICLAUS jointly and severable liable with Defendant TIBERIU DANET, for restitution in the amount of $842,483.93 consistent with its Amended Order of Restitution dated December 22, 2020.

IV. GUIDELINE CALCULATION OF SENTENCE

The district court's task is to impose a sentence that is sufficient, but "not greater than necessary" to comply with the factors set forth in 18 U.S.C. § 3553(a)(2). 18 U.S.C. § 3553(a). In achieving this task, district courts are to consider the Sentencing Guidelines *together* with the statutory factors set forth in § 3553(a). *See United States v. Booker*, 543 U.S. 220, 246 (2005).

The government argues that in using this discretion, on remand, there is nothing in the Sixth Circuit's remand that suggest the original sentences, which fall squarely in the new Adjusted Offense Range, would run afoul of § 3553(a) analysis. The government further argues that no additional departures are warranted or appropriate; the departure from 48 to 43, and again from 43 to 38 were taken at the original sentence to manufacture a range for each defendant that provided ranges that were inclusive of the 240-month statutory maximum while also satisfying the goal of § 3553(a) to reach a sentence adequate, but not greater than necessary, to punish a defendant. Since the Adjusted Offense Level on remand is *37*, one level lower than the agreed-to

adjustment at the original sentencing, and still inclusive of 240 months (210-262 months), no additional departures are necessary or appropriate given the Court's findings of fact establishing the proper calculated enhancements.

A. Co-Conspirator Liability Under the Guidelines

The Defendants were convicted of four counts which were charged explicitly as conspiracies. As for the remaining twelve convictions for wire fraud and five convictions for aggravated identity theft, both Defendants should also be liable for the entire criminal scheme as co-conspirators. Pursuant to the Sentencing Guidelines and well-established principles of conspirator liability, and consistent with how NICOLESCU and MICLAUS were charged in the Indictment, a conspirator is deemed responsible for the acts of his or her co-conspirators, if those acts were foreseeable and in furtherance of the conspiracy:

> Unless otherwise specified, (i) the base offense level where the guideline specifies more than one base offense level, (ii) specific offense characteristics and (iii) cross references in Chapter Two, and (iv) *adjustments in Chapter Three,* shall be determined on the basis of the following:
>
> > (1)(A) all acts and omissions committed, aided, abetted, counseled, commanded, induced, procured, or willfully caused by the defendant; and
> >
> > (B) *in the case of a jointly undertaken criminal activity (a criminal plan, scheme, endeavor, or enterprise undertaken by the defendant in concert with others, whether or not charged as a conspiracy), all reasonably foreseeable acts and omissions of others in furtherance of the jointly undertaken criminal activity,*
>
> that occurred during the commission of the offense of conviction, in preparation for that offense, or in the course of attempting to avoid detection or responsibility for that offense....

U.S.S.G. § 1B1.3(a) (emphasis added).

Using this standard to determine the co-conspirator liability of each defendant, it is clear that both NICOLESCU and MICLAUS took definite and certain physical action that clearly and unequivocally supported the objective to use internet auctions to defraud victims, transfer money

overseas to evade detection, and use computer intrusions and theft of actual identities to perpetuate the criminal enterprise. Indeed, each defendant in this case had certain tasks that he performed that were necessary to achieve the objects of the conspiracy. There has been no change in this interpretation since sentencing and, as such, the government reaffirms its position that each defendant is responsible for the criminal conduct of the other as co-conspirators.

B. The Proper Advisory Base Offense Guideline Range Calculation is Level 37 (210-240 Months)

With respect to Counts 1 through 15 and 21 of the Indictment, the Pre-Sentence Report (PSR) states that these counts are grouped as one count based on common conduct and characteristics under U.S.S.G. § 3D1.2(c) and (d). Therefore, the Base Offense Guideline Range will be calculated using conspiracy to commit money laundering as the controlling conviction.[3]

1. Base Offense Level of 7

The base offense level for 18 U.S.C. § 1956(h) is U.S.S.G. § 2S1.1(a). That Guideline directs the use of the offense level for the underlying crime, which would be U.S.S.G. § 2B1.1 (a)(1). Thus, the base offense is **7**. U.S.S.G. § 2B1.1 (a)(1).

2. A Conservative Loss Amount of Between 3.5 and 9.5 Million Dollars

Assuming the order of remand is a limited remand, the government believes the conservative calculation of a loss value of 3.5 to 9.5 million dollars is appropriate.

a. Banks *is inapposite in this case.*

The government argues that the holding in *United States v. Banks*, 2022 WL 17333797 (3rd Cir. Nov. 30, 2022) is inapposite on remand in this case. The *Banks* holding contemplated

[3] The government recognizes that the following discussion is largely, but not entirely, a recitation of a previously filed Sentencing Memorandum, but believes that incorporating prior arguments, augmented by additional arguments is necessary to preserve its position in any future appellate practice.

the difference between *intended* loss and *actual* loss, including a lengthy quote from a Sixth Circuit case, *United States v. Riccardi*, 989 F.3d 476, 486 (6th Cir. 2021), on the semantics of the two words. In this case, the record is clear that the loss used to calculate loss amount was *actual* loss, not intended loss. In fact, as discussed below, the loss amounts were not only based on actual complaints by victims *after* they fell victim to fraud perpetrated by the Bayrob Group, and confirmed by reviewing records of profits realized by Bayrob Group members, but a conservative method to calculate those losses was used. Using the plain meaning and understanding of what an actual loss would be, the government argues that a loss actually sustained by a victim, and a loss actually converted by the defendant, falls comfortably in any parsing of the *Banks* analysis.

Indeed, using the logic of what constitutes a loss as testified to by SSA Macfarlane, the defense further citation to *United States v. McKinney*, No. 22-CR-20249 (E.D. Mich. Dec. 9, 2022), actually augers in the government's favor. The *McKinney* court found a difference between stolen funds placed in a bank account versus a portion of those funds withdrawn from that account, seemingly holding that there is a difference between stolen funds that are held after being stolen and those immediately converted. The government believes *McKinney* is not applicable here and even if it were, based on the Defendants' laundering of funds from domestic accounts to foreign accounts, and then again to cryptocurrency, they more than adequately converted any loss into a loss that *McKinney* would define as "actual losses."

If actual loss is calculated as the loss suffered by the victim, not potentially suffered, as is suggested by the *McKinney* court, then using SSA Macfarlane's method of calculating loss using amounts provided by *actual* victims reporting *actual* losses to law enforcement, eBay Fraud monitors and other reporting sources is consistent with *McKinney's* tabulation only of monies actually converted by defendants. However, such analysis is of no moment at this sentencing

because the loss amount was properly calculated using established Sixth Circuit precedent and the record does not suggest that the finding of loss was based on anything but calculations of *actual* loss derived from reliable records.

b. Loss was properly calculated to be between 3.5 and 4.5 million dollars of actual loss

Pursuant to § 2B1.1 (b)(1), a loss amount must be calculated. The PSR uses the most conservative calculation of a loss amount of between 3.5 and 4.5 million dollars based solely on eBay fraud. The government has consistently used this conservative estimate, which is based on an analysis of (a) the amounts.xls spreadsheet which co-conspirator Valentin Danet accidentally sent to his brother TIBERIU DANET in unencrypted form; (b) IC3 complaints; and (c) victim statements. (R. 230: Hearing Transcript, PageID 3201-05), Ex. 1741, *see also* Exs. 1429 and 1165. The government avers that this calculation satisfies any analysis under *Banks* both because it is supported by testimony from SSA Macfarlane at the original hearing as to how that loss calculation was achieved, but also because that represents *actual* losses suffered by victims, not mere intended loss. (R. 230: Hearing Transcript, PageID 3201-05), Moreover, even assuming *arguendo* that the losses testified to by SSA Macfarlane are based on extrapolated totals, those totals are still calculated on actual recorded complaints and figures represented as monies lost by actual victims or realized and converted by the Bayrob Group. *Id*. Simply, using the most plain meaning definition of the phrase "actual loss," SSA Macfarlane's calculations were based on representations of claims of monies actually missing from victims' bank accounts as a result of entering into fraudulent transactions with NICOLESCU and MICLAUS; not contracted agreements, not scheduled payments, not credit obligations, actual money sent by victims to NICOLESCU, MICLAUS, and the rest of the Bayrob Group as a result of their fraud scheme.

And indeed, at sentencing SSA Macfarlane testified that the loss amount was, at a conservative minimum 3.5 million and that the IC3 complaints represent only about one-third of the identified victims of the eBay scheme and, thus, it could be reasonable to extrapolate that loss amount from the eBay fraud alone to be as high as 10.5 million dollars. *Id*. This range of between 3.5 and 10.5 million dollars is entirely appropriate and within the deferential determination afforded the sentencing court under § 2B1.1 Application Note 3(C).

Thus, if the Court were to stop at this loss calculation in deference to the most restrictive reading of the Sixth Circuit's limited remand and *Banks*, the actual loss value would be at least 3.5 to 4.5 million dollars.

However, if Defendant NICOLESCU's brief is followed, such a restrictive reading is not mandated by the Sixth Circuit, nor precluded by *Banks*, and in fact, NICOLESCU and MICLAUS' offense conduct allow for a finding of actual loss consistent with the original findings by this Court. As calculated below, if remand is not limited, then the loss amount could reach a Guideline calculation as high as level **22** based on losses totaling over 30 million dollars. *Id*. at 3204-05.

c. Stolen Credit Cards Used by the Bayrob Group

The number of credit cards and access devices stolen during the course of the enterprise must be assigned a loss value. In Application Note 3(F), the sentencing court is to give every stolen credit card or access device a value "not less than $500 per access device." Id. Based on databases and other files found within the Bayrob Group's command and control infrastructure, it is clear that the group stole and trafficked over 25,000 credit cards and used or sold them over various forums.

Before proceeding further, the government argues that the *Banks* opinion, while not applicable to an actual loss calculation above, is likewise inapposite to the following analysis of loss based on credit card and credential fraud. The government argues, and *Banks* maintains a stony silence that is cold comfort to the defendants, that the assignment of minimum values as loss for credit cards and credentials is not only proper, but in this sort of case of an urgent import. The government argues that this case presents a scenario that supports finding a minimum loss amount for each credit card and credential based on the purpose those cards and credentials were stolen. The government argues that is entirely consistent with how these defendants used stolen cards or credentials, both as sources of revenue from which they could promote and support their criminal infrastructure through the purchase of domain names and server space, and as a source of revenue generation through the periodic sale of credentials on darkweb marketplaces.

Were the defendants merely using stolen credentials for personal enrichment and personal use an inquiry into the propriety of assigning a set loss amount *may* be warranted, this was certainly not the case with NICOLESCU and MICLAUS, their use of stolen credit cards and credentials was to further their criminal activities, and as such, they attached a value to the credentials above that of mere largess, they treated them as a tools for their ongoing criminal enterprise. Thus, because their use of the cards and credentials was not for potential personal gain, but ongoing use to further a criminal scheme, a corresponding loss value, in this case $500, is appropriately applied to reflect their inevitable conversion to either promote the Bayrob infrastructure or generate illicit revenue on the darkweb.

In his plea agreement, DANET admitted that the group "collected and used more than 500 stolen credit cards through our scheme." (R. 99-1: Danet Plea, PageID Paragraph 113) The

term "used," for this analysis means cards used to register false domain names, rent server space, or pay for other monthly or recurring fees needed to support the Bayrob infrastructure. Based on a review of the various databases titled "cc tables" SSA Ryan Macfarlane estimates this number to be at least 800. His estimation is very conservative and based on a review of the "cc tables"[4] that identified over 670 unique credit card numbers with associated notes about their use. It also includes credit cards assigned record identification numbers created and assigned by the Bayrob Group which totaled 773. His analysis also revealed that over time the Bayrob Group added and deleted active cards from the cc tables database; accounting for these additions, a conservative number of cards actually used for infrastructure support over the ten years of the enterprise is **800**. (R. 230: Hearing Transcript, PageID 3205-08, 10-12),

d. Stolen Credit Cards on Alphabay Attributed to Vendor Cvv2land

In an interview with Bayrob Group member Valentin Danet, Danet told investigators that the group sold over 10,000 cards on Alphabay to his knowledge. SSA Macfarlane's investigation confirmed the Bayrob Group was selling stolen credit cards harvested from infected computers and the computers themselves as proxies, under the Alphabay vendor "cvv2land". SSA Macfarlane confirmed the group was selling both credit cards and proxy services in a number of undercover buys from the vendor "cvv2land" which were then identified in evidence collected from Bayrob servers. SSA Macfarlane identified over 1700 credit card transactions in the seized databases, and confirmed through analysis there were other transactions not listed in the database tables. Additional analysis showed a larger subset of credit card numbers had been collected

[4] Testimony from SA Macfarlane, Liam O'Murchu, and members of the Bayrob Group established the reliability of these tables.

from infected systems in various states of processing, well over **5,000**, at the time of the arrest and takedown. *Id*. at 3210-12.

e. Other access credentials

The Bayrob Group was also collecting a large number, over 70,000 in one database alone, of online service accounts and passwords, from services such as Yahoo and Facebook. Initially, these accounts were used to send additional malware using stolen accounts, and in 2016 the group started selling account information based on files found on one of the seized Bayrob servers. For example, one server had multiple related files, such as a file named "accounts_sold.txt", containing over 2500 accounts from multiple service provides such as Amazon, Google, Yahoo, Paypal and Facebook. SSA Macfarlane's analysis found that these accounts were likely sold through a source different than Alphabay. Additionally, at the time of arrest, the Bayrob Group was actively collecting Wells Fargo accounts, exploring collecting Bank of America accounts, and may have been selling banking accounts as well based on established behavior.

Analysis showed it was completely reasonable the Bayrob Group sold over **10,000** credit cards collected from systems infected by the Bayrob Group, and this number also accounts for infected proxies, and accounts collected from the botnet being used as "access devices" as defined in the Application Notes. *Id* at 3210-13.

f. Pre-existing Stolen Credit Cards Possessed by the Bayrob Group

Finally, because this investigation spanned ten years, and because evidence was collected throughout that time period using a variety of collection methods, SSA Macfarlane was able to track stolen credit cards through the evolution of the enterprise. Thus, in addition to the four-above identified groups of stolen cards, he was able to isolate a compress file from one of the

earliest Command and Control servers used by NICOLESCU, MICLAUS and the rest of the Bayrob Group named "10000cards.7z" which contained over **10,000** credit cards *in addition* to those already delineated. *Id*.

Thus, doing an accounting using the numbers compiled, tracked and saved by the Bayrob Group, the group conservatively possessed or used at least **25,000** credit cards themselves to pay for their own criminal infrastructure, or sold or attempted to sell them on the Dark Web, and gather and/or sold over 70,000 account credentials. The loss value for stolen credit cards alone would be more than 12.5 million dollars. *Id*. at 3208-13.

Regardless of how much loss the Court assigns the stolen credentials, based on the actual eBay loss calculations the Defendants' § 2B1.1 (b) loss amount is between 3.5 and 9.5 million dollars, well within § 2B1.1 (b)(1)(J)'s range of 3.5 and 9.5 million dollars, for an addition of **18 levels**.

If anything, this is a conservative estimate of total loss, given the ten-year life span of the scheme, the Defendants' extraordinary efforts to conceal their activities online (severely limiting the government's ability to identify victims and loss), the Defendants' ability to use or sell on the black market stolen information from over 400,000 infected computers, and Defendants' refusal to decrypt their computers (which would likely contain a treasure trove of information about victims and loss).[5] If a revised number on general remand is warranted, the government asserts

[5] Given that the Defendants have already been convicted of all 21 counts, their continuing refusal to decrypt their hard drives suggests that the information on their hard drives will (a) reveal a significantly higher loss amount; and/or (b) provide the government with access to Defendants' criminal proceeds, which could be used to compensate many of their victims.

that the loss value is comfortably over 30 million dollars, and the adjusted enhancement would properly be **22.**[6]

3. There Were In Excess of Ten Victims[7]

Given that the Bayrob Group infected more than four hundred thousand computers, the two levels for in excess of ten victims assessed in § 2B1.1 (b)(2)(A) grossly understates the number of victims harmed by the Bayrob Group. Although the government cannot seek additional levels for those hundreds of additional victims under this subsection, the impact victims felt as a result of this crime is demonstrated in the dozens of victim impact statements submitted by the government and the testimony of victims during trial.[8] However, the impact statements are replete with victims recounting how they were financially injured. This scheme targeted hundreds of thousands of victims wantonly and without regard to their financial wherewithal. And at trial William Scott Hannon and Ashley Parton gave testimony that rose to the level of "substantial financial hardship" as defined in Application Note (4)(F). Hannon testified that he declared bankruptcy and Parton had her bank accounts frozen and was arrested and had her house searched as a result of being an unwitting money mule.

[6] For consistency, the government will continue to calculate its recommended sentence using the 37 level remanded by the Sixth Circuit. The government recognizes that even if a loss value of 22 was assigned, as in the original sentencing the defendants would be assigned an Adjusted Level 38 because it is the first range that is inclusive of the 240 month statutory maximum.

[7] The Enhancements discussed in subheadings 3, 4, 6 and 7 were not challenged on appeal.

[8] As of July 22, 2019, there were 88 victim impact statements received by the government and submitted to the U.S. Probation Office. Almost all of the victim impact statements include statements by victims that describe the loss of thousands of dollars, feelings of guilt for being scammed, and a loss of confidence and trust in the internet. Many victim impact statements also state that after being defrauded the victim felt anxious, depressed, or other manifestations of being victimized, like loss of sleep or change in mood.

The Defendants not only created a scheme to steal and use credit cards, as demonstrated in Exhibits 1204 and 1429, they created infrastructure to streamline the victimization, Ex. 1149, and they could even see new credit card data if the victim replaced the stolen card. *See, e.g.,* Ex. 1137. As discussed in greater detail in Section IV, SSA Macfarlane's analysis of databases containing stolen credit cards and victim credentials is at least 25,000. If, in crafting an appropriate but not greater than necessary sentence, the Court needs to identify an interest underrepresented by the Guidelines, the government suggests it look here. The number of victims harmed far surpasses a mere **2 level** increase under § 2B1.1 (b)(2)(A).

4. The Defendants Carried Out the Scheme From Outside the United States

Pursuant to either § 2B1.1 (b)(10)(B) or (C), two levels should be added to the base offense level. Neither defendant had ever traveled to the United States prior to the extraditions and the investigation clearly traced all internet traffic back to Romania, where Defendants were arrested. Additionally, Bogdan Antonovici, Donna Wolfe, and Ashley Parton clearly and unequivocally explained the money mule process that moved funds from domestic victims to the pockets of NICOLESCU and MICLAUS overseas. A **2 level** increase for either (B) or (C) must be made.

5. The Defendants Produced and Trafficked in Authentication Features and Possessed More Than Five Authentication Features Produced or Obtained by Unlawfully Through the Use of Another Means of Identification

As discussed before, the Bayrob Group relied on the use of stolen identities to support and perpetuate their criminal enterprise, which had one goal of obtaining more stolen identities. The two-level increase under § 2B1.1 (b)(11)(B)(ii) or (C)(ii) is appropriate here because they used stolen identities to mask their true identities and intentions in order to dupe unsuspecting online consumers. As noted before, and supported by the testimony of members of the Bayrob

Group, the Bayrob Group constantly used stolen credit cards and identities to register domain names, servers, and virtual private networks to further the scheme and mask their identities. *See, e.g.,* Exs. 2079 and 1441. Likewise, in order to lend the air of legitimacy, they used stolen identities, bank account information, and credit cards to list auctions, communicate with buyers, and recruit money mules. Exs. 2078 and 2079. The necessity of producing and acquiring stolen identities to use in their scheme was so constant that, as with the number of victims impacted by this crime, a two-level increase fails to describe the importance of using the identity of others was to the scheme. This is also reflected in the fact that even using subsection (C), **2 levels** appears insufficient; the number of victims exceeds five by a multiple of thousands based on the databases created, maintained, and used by the Defendants. *See, e.g.,* Ex. 1149.

6. The Defendants Were Convicted for 18 U.S.C. 1956(h)

Going back to § 2S1.1, the Defendants should be levied an additional **2 levels** because, as directed by § 2S1.1 (b)(2)(B), they were convicted of money laundering conspiracy, an offense included in 18 U.S.C. § 1956.

7. The Defendants Used Sophisticated Laundering Techniques

The PSR more than adequately summarizes the multiple layers of sophistication used by the Bayrob Group to launder funds pursuant to § 2S1.1(b)(3). It should be noted, however, that this sophistication enhancement is different than the one in § 2B1.1 or the Chapter 3 enhancement for use of a special skill. As delineated in Application Note 5(A)(i) and (iii), this enhancement is specifically for the techniques used to launder the funds—not to cause the loss or theft. Therefore, because the Defendants recruited money mules using fictitious companies, and registered those companies using stolen credit cards and identities, subsection (i) is clearly met.

Moreover, based on the testimony of Bogdan Antonovici, subsection (iii) also applies because Defendants arguably used at least six levels of subterfuge to launder the proceeds of their crime:

- Level 1: Defendants created fictitious U.S. companies by registering domain names with false information, creating legitimate seeming corporate websites, and using stolen credit cards to purchase disposable email accounts, phone numbers, and fax numbers.

- Level 2: Defendants placed ads on job boards to recruit mules to wire money from an unwitting victim in the United States to Europe. Sometimes these ads purported to seek "wire transfer agents," but in other instances the Bayrob Group pulled a complete bait-and-switch, advertising a totally unrelated position, such as sales manager. For victims who were already infected with the Bayrob Trojan, the Bayrob Group would inject advertisements into web browsers which would make it appear that Google and Yahoo were seeking to hire "wire transfer agents."

- Level 3: U.S.-based money mules would open up a new bank account to receive wire transfers. Once a victim wired money to the account, the U.S. mule would quickly withdraw the funds, and use a Western Union to wire the money to a European money mule. The U.S. money mule would then often be directed to close the U.S. bank account.

- Level 4: A European money mule would use a fake ID to pick up the funds at a money transfer station in Europe. The European mule would then transfer the money to Antonovici's contact who was based in Germany.

- Level 5: Antonovici's contact would directly or indirectly provide the money to Antonovici, who also used accounts in other peoples' names to receive the money.

- Level 6: Antonovici ultimately withdrew they money using a fake identification and surreptitiously delivered it in cash to MICLAUS (or in some instances NICOLESCU or DANET), who received the money BMW window to BMW window.

Because of these sophisticated techniques, both technically sophisticated and densely layered to create almost impenetrable anonymity, the additional **2 levels** pursuant to § 2S1.1(b)(3) should be applied.

Before applying Chapter 3 enhancements the Defendants' Base Offense Level is **33.**

C. Applicable Chapter 3 Enhancements

1. Both Defendants Were Leaders and Managers in the Scheme

One of the most remarkable and chilling truths about this case is that the Bayrob Group developed their virus, infected hundreds of thousands of computers, stole millions of dollars and thousands of identities, and did it over more than a decade with only a handful of core co-conspirators. While they bragged to victims that they ran the "organized crime" group with only about five people, Exs. 1324, 1327 and 1328, in reality their Romanian group included at least ten individuals posting auctions, updating code, and laundering money including: NICOLESCU, MICLUAS, TIBERIU DANET, Valentin Danet, Catalin and Valentin Dima, and Marius Matei, as well as several other Romanian group members who did not testify at trial, a number of European-based money mules who were a necessary cog in the laundering process, and U.S.-based money mules, two of whom, Donna Wolfe and Ashley Parton, testified against the Defendants. Simply, the number of lower-level members of the group supervised, managed, and controlled by NICOLESCU and MICLAUS numbered well above the five suggested by U.S.S.G § 3B1.1(a).

Moreover, Application Notes 3 and 4 firmly place both Defendants within the top definition of leader or organizer because the criminal enterprise was "otherwise extensive," and their roles were those of people in positions of authority and control. The success and promulgation of the scheme depended on the constant infection of computers, which, in turn, provided profit that supported the criminal infrastructure. Both of these factors were closely managed and controlled by the three core members of the Bayrob Group, NICOLESCU, MICLAUS, and DANET. While it is convenient to ascribe certain tasks to each of the three core members, in practice, all three were involved with each step of the scheme and were necessary to

its long term success. Thus, while there is evidence that MICLAUS (under the nickname of "min") posted and managed a larger number of auctions than other members (*e.g.,* Ex. 1144), NICOLESCU was also active in that part of the scheme. *See, e.g.,* Ex. 1141. Likewise, although NICOLESCU was the architect of the Bayrob Virus, MICLAUS certainly had the skill to use the underlying infrastructure (*e.g.,* Ex. 1747), and was competent in managing it.

Applying these facts to scenario proposed in Application Note 3, the similarities are striking. As suggested in the Note, if as few as three Defendants are engaged in a fraud scheme dependent on many unknowing participants or services, U.S.S.G. § 3B1.1(a) may be satisfied. In this case, there were at least ten core members of the Bayrob Group as well as scores of U.S. based and European money mules. Further, Defendants used the hundreds of thousands of unknowing and unsuspecting computers to advance their scheme, and used credit cards and credentials of hundreds of more unknowing victims to support the infrastructure of the scheme.

Likewise, the conduct of NICOLESCU and MICLAUS fall squarely in the definition of leader, organizer, and manager in U.S.S.G. § 3B1.1(a) App. Note 4. While Matei, both Danets and Dimas, and other Bayrob members cycled in and out of the Group, there were two constant members, NICOLESCU and MICLAUS. Their constancy is reflected in the fact that NICOLESCU and MICLAUS shared profits, shared equipment (*e.g*., Exhibit 1415), and even rented apartments together. Unlike DANET, who left the group for a while, both NICOLESCU and MICLAUS remained active and sought replacements for DANET. As the scheme evolved to focus on cryptocurrency mining, both Defendants had evidence that they were engaged in cryptocurrency mining (e.g., Poloniex, Bter, Ypool, Burst, etc.) on their phones, computers, and even in their social media posts. *See, e.g.,* Ex. 1448.

Moreover, NICOLESCU and MICLAUS were able to maintain compartmentalized control over each aspect of the enterprise by limiting interactions between other members of the group. For instance, with MICLAUS taking the lead, they were the only two members to deal with Antonovici, who in turn, managed the European mule network. However, the U.S.-based mule network fell under the control of various other members, who were under the authority of NICOLESCU, not Antonovici. The Command and Control server was similarly compartmentalized; while each Bayrob Group member had their own workspace (*e.g.,* Ex. 1126), it was clear that NICOLESCU developed much of the malware's functionality, and MICLAUS deployed it most commonly through auctions. *See, e.g.,* Ex. 1144.

Thus, because both NICOLESCU and MICLAUS exercised authority and control over more than five people in an ongoing and extensive enterprise, both are deserving of a **4 level** enhancement under U.S.S.G. § 3B1.1(a).

Thus, after Chapter Three adjustments, the correct Adjusted Offense Level is **37**.

D. There are No Applicable Departures

"The defendant bears the burden to prove by a preponderance of the evidence that the circumstances of his or her case warrant a downward departure." United States v. Holz, 118 Fed. Appx. 928, 931-32 (6th Cir. 2004) (*quoting* United States v. Lipman, 133 F.3d 726, 730 (9th Cir. 1998)). *See also* United States v. Bostic, 371 F.3d 865, 874 (6th Cir. 2004) (defendant bears burden of proving a downward departure is warranted).

When determining whether a Guidelines-based departure is justified, a district court must consider the following factors:

> (1) What features of this case, potentially, take it outside the Guidelines' 'heartland' and make of it a special, or unusual, case? (2) Has the Commission forbidden departures based on those features? (3) If not, has the Commission encouraged departures based on

> those features? (4) If not, has the Commission discouraged departures based on those features?

United States v. Erpenbeck, 532 F.3d 423 at 440 (6th Cir. 2008) (*citing* Koon v. United States, 518 U.S. 81, 95 (1996)).

Additionally, only certain grounds for departure are permissible. Pursuant to U.S.S.G. § 5K2.0(d)(1), the Court may not depart from the applicable Guideline range for a number of factors, including the defendant's national origin, religion, socio-economic status, or his/her disadvantaged upbringing. Moreover, while a defendant's role in the offense is relevant in determining the applicable guideline range, it is *not* a basis for departing from that range. *See* U.S.S.G. § 5K2.0(d)(3).

The Guidelines also identify a number of discouraged factors for granting a departure. A departure under these factors may be granted, but only under extraordinary circumstances. *See* U.S.S.G. Chapter 5, Part H (Specific Offender Characteristics). These factors include, *inter alia*, age, mental and emotional conditions, and family ties and responsibilities. *Id*.

While Defendants apparently told Probation that their childhoods involved certain hardships, none is so severe as to raise to the level of "extraordinary circumstances." Further, none of Defendants' claims are in any way verifiable, and Defendants have shown themselves to be anything but credible or trustworthy. Accordingly, no downward departure should be granted, and the advisory Guidelines range of life imprisonment should be imposed.

E. Total Adjusted Base Offense Level

There is no reduction for Acceptance of Responsibility because Defendants did nothing to accept responsibility. Indeed, since being sentenced on December 16, 2019 until now, neither Defendant has exhibited *any* inclination to accept responsibility.

With the new adjusted calculations, the Defendants' Adjusted Base Offense Level is **37.** Defendants are statutorily capped at 20 years for most of their convictions,[9] and therefore their final adjusted range should be **Level 37, 210 to 240 months**. The government is, without hesitation, recommending the same sentence originally handed down by this Court for NICOLESCU and MICLAUS.

Calculating an offense level such as this, however, is not a mere intellectual exercise in this case on remand. NICOLESCU and MICLAUS, used not only sophistication and skill to evade detection and develop and evolve a criminal enterprise of staggering efficiency and corruptness, but that they executed it hundreds and thousands of times over and over in the hopes of victimizing as many people as possible. The final offense level is so high because Defendants went about committing their crimes with a calculation and ruthlessness that warrants such a result.

Moreover, defendants intentionally executed their criminal scheme in a manner meant to inflict the maximum amount of harm to the victims in large part because they were both patient, brazen, and sadistic. Unlike schemes that charge the maximum limit on a credit card, these Defendants used the cards incrementally and over time to support the growth of their scheme. They created software that organized the cards, made repeated harvesting of data efficient and automated, and thus were able to avoid detection for more than ten years. As NICOLESCU assured DANET in an encrypted chat, "now we really have power...and power is more important…[but soon we will have] both money and power." Ex. 367, pg. 733, lines 26978-26984.

[9] The sentences for the five convictions for 18 U.S.C. § 1028A will be discussed below.

As explained above, the Adjusted Base Offense Level is high because of Defendants' comprehensive criminal conduct. All of the aggravating enhancements are directly attributable to NICOLESCU and MICLAUS' years of methodically and unrelentingly growing, evolving, and exploiting the full criminal potential of the Bayrob Trojan.

F. One 1028(A) Aggravated Identity Theft Sentences Should Run Consecutively

The government firmly believes that a sentence in which one two-year term of incarceration for aggravated identity theft run consecutively is not greater than necessary to punish both Defendants. At trial, five victims from the Northern District of Ohio personally appeared and testified about the fraud committed on them by the Defendants.[10] In addition to the financial loss, their victimization extended to having to open new business or personal accounts, personal embarrassment, loss of trust in e-commerce and the internet, and costs associated with buying new computers or wiping existing hardware of the Bayrob Trojan. These five victims, along with the other victims who testified, and the dozens more who wrote victim impact statements, cannot be made whole by any sentence. The embarrassment, loss of time and money, and lack of trust or growing cynicism toward the internet and all electronic transactions is part of the purpose of providing individual, consecutive punishment for each and every victim of aggravated identity theft serves.

While the Defendants viewed their criminal enterprise as a faceless, remote, and abstract means to gain power, steal money, and perfect their art, the effects of their actions in Romania were felt directly here, in the Northern District of Ohio, and elsewhere. While the Defendants saw the Bayrob Trojan as a means to obtain power while lining their pockets in order to pursue

[10] Ms. Muhlenkamp testified on behalf of her husband, who died during the pendency of the investigation and thus was not able to personally confront the Defendants who defrauded him of thousands of dollars.

the idles and hobbies of the skydiving, motorcycle collection, BMWs, international travel, and purchasing expensive electronics, Ohio victims such as Clint Bertke were inconvenienced for years afterwards. Likewise, while NICOLESCU hoarded millions of dollars in Bitcoin (which he still has not made accessible to the government or victims), victims like Donald Wertz were working multiple jobs to help care for sick family members.[11]

The victims who testified are not abstractions or simply bank accounts to hack into. They are citizens of the Northern District of Ohio; they work hard for their money; and they hoped to use some of that extra hard-earned income on goods that reminded them that an honest day's work is rewarded. Instead, NICOLESCU and MICLAUS, two criminals who used their superior intelligence and computer skill to prey on innocent victims instead of finding honest work, took advantage of these people for their own ego and selfish gain. And they created malware that was able to do it again, and again, and again, hundreds of thousands of times over and over.

IV. 18 U.S.C. Section 3553 Factors

As noted above, the sentencing court is required to "impose a sentence sufficient, but not greater than necessary, to comply with the purposes set forth" in Section 3553(a)(2), including "the need for the sentence imposed: (A) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense; (B) to afford adequate deterrence to criminal conduct; (C) to protect the public from further crimes of the defendant; and (D) to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner." 18 U.S.C. § 3553(a)(2).

[11] In fact, even on the day of his testimony Mr. Wertz came directly from an over-land hauling job to testify before having to leave to take a family member for medical care.

In fashioning a sentence that is sufficient, but not greater than necessary to comply with the purposes set forth in Section 3553(a)(2), the Court must also consider: "the nature and circumstances of the offense and the history and characteristics of the defendant" under 18 U.S.C. § 3553(a)(1); "the kinds of sentence and the sentencing range established for . . . the applicable category of offense committed by the applicable category of defendant as set forth in the guidelines" under 18 U.S.C. § 3553(a)(4)(A); "any pertinent policy statement . . . issued by the Sentencing Commission . . . " under 18 U.S.C. 3553(a)(5)(A); and "the need to avoid unwarranted sentence disparities among Defendants with similar records who have been found guilty of similar conduct . . . ." under 18 U.S.C. § 3553(a)(6).

While it is not necessary for the district court to "engage in a ritualistic incantation of the § 3553(a) factors," its reasoning should be "sufficiently detailed to reflect the considerations listed in § 3553(a) and to allow for meaningful appellate review." *United States v. Moon*, 513 F.3d 527, 539 (6th Cir. 2008) (internal quotations and citation omitted). Simply stated, a sentencing judge is not required to "expressly state each of these factors at sentencing." *United States v. Mayberry*, 540 F.3d 506, 518 (6th Cir. 2008). However, if the district court determines that "an outside-Guidelines sentence is warranted, [it] must consider the extent of the deviation and ensure that the justification is *sufficiently compelling* to support the degree of the variance." *United States v. Erpenbeck*, 532 F.3d 423, 437 (6th Cir. 2008) (*quoting United States v. Gall*, 128 S. Ct. 558, 597) (2007) (emphasis added). A variance "based on a policy disagreement with the Guidelines . . . may be entitled to less respect" and be "suspect" on appeal. *Spears v. United States*, 128 S.Ct. 586, 599 (2007); *see United States v. Herrera-Zuniga*, 571 F.3d 572, 585-86 (6th Cir. 2009).

A. The Need to Reflect the Seriousness of the Offense, Promote Respect for the Law and Provide Just Punishment for the Offense

Criminals should not believe that cybercrime is a victimless crime because they cannot physically see their victims, or because a keyboard is used in place of gun. In this case, and in more and more cases, the danger of cybercrime is that its scope is wider, and it reaches much further, than traditional fraud schemes. The ability for Defendants to use malware and botnets exponentially increases the number of potential victims. And as seen in this case, cybercriminals are also evolving in how they can mine victims' data for more than just a single credit card number. The Bayrob Group is noteworthy, not just because they sent more spam in 2016 than any other criminal group worldwide, but because they comprehensively mined and re-mined their victims' data for any and all valuable information, including user names, passwords, credit card information, social security numbers, bank account information, etc. Their sentence should reflect the comprehensive and complete exploitation of their victims.

A running theme through the Defendants' interactions with victims is their feeling of superiority and entitlement over U.S.-based victims. *See, e.g.,* Exs. 1325 and 1329. This misguided air of superiority even extended to their taunting of Symantec and other investigators. *See e.g.,* Ex. 1450. Given their belief that they were ensconced behind seven proxies ensuring their anonymity, the Bayrob Group believed their geographic and technological distance would protect them forever. Such hubris must be proportionately punished and made an example. NICOLESCU and MICLAUS believed that they could defraud millions of dollars from Americans and use it for their own leisure and indulgences. Clearly, they believed that being overseas and being more technologically sophisticated than anyone else, they would never get caught. However, just as the internet has made it easier for transnational cybercriminals to find far-flung victims, it also has given agencies such as the FBI greater ability to expose criminals

wherever they may be and bring them back to face justice. If anything, since their original sentencing, the world of cyberfraud has become more complex and more incipient.

As discussed below, the defendants were calculating, unrepentant, and caused great harm – financial and personal – to their victims. If anything, the tools and practices used by the Bayrob Group were mere foreshadows of the current and evolving threat landscape in the cyberworld. One of the hallmarks of the Bayrob Group was its evolution of their malware trojan to adapt and evade detection. This ability is seen in pernicious forms of malware, ransomware and zero-day worms that are targeting healthcare facilities, energy providers and schools around the world. Likewise, the database mining and information harvesting used by Bayrob in its world-wide botnet is now a common feature of most ransomware malware suites and attack software. Simply, the Bayrob Group was a harbinger of the cyber-attacks that are now crippling vital infrastructure around the world and early generation architects such as these defendants of such malware should not be given lighter sentences on remand.

B. The Need for the Sentence to Afford Adequate Deterrence

The consideration of deterrence in this case is both for the Defendants and those seeking to take their mantel. As a result of new technology, the barriers to entry for new cybercriminals has become extraordinarily low. Even unsophisticated would-be criminals can now simply purchase, lease, or hire, malware, coders, botnets, money mules, bullet-proof hosters, and everything else they need to commit their crimes. Moreover, the rewards for cybercrime have increased as individuals, businesses, and government agencies now place more and more sensitive and valuable data online, and as there are now dark markets and cryptocurrency exchanges which criminals can use to easily and securely monetize their ill-gotten gain. At the same time, the government's ability to deter cybercrime has been diminished as cybercriminals

increasingly attack U.S. victims from foreign countries, using now-readily available technology to effectively conceal their identities. This case is the perfect example—it took the U.S. government and the private sector 10 years, thousands of hours, and millions of dollars to apprehend just these three cybercriminals. Given that foreign cybercriminals engage in this conduct, in part, because they believe it is very unlikely that they will be caught and brought to justice, in the rare cases that it does happen, the sentence must be particularly severe if it is to have any deterrent effect at all. In other words, if the likelihood of being caught is relatively low, the cost of being caught must be proportionately high, if there is to be any material deterrent effect.

Receding into the shadows are the days of individual hackers acting alone. Instead, the trend today is for more coordinated collection, analysis, and distribution of data as it is stolen. While NICOLESCU and MICLAUS may represent an especially successful model of this new evolution in crime, they are simply the tip of the spear of what is coming, therefore, their sentences should be a clarion call to those thinking of following in their footsteps, whether in Romania or elsewhere in the world.

Based on the testimony of the former members of the Bayrob Group, and based on the other evidence presented in Court, the defendants in this case were compelled by their desire to amass the largest botnet of infected computers, continue to expand the functionality and scope of their criminal enterprise, and a lust to achieve both "money and power" through the use of their criminal enterprise. *See* Ex. 367, pg. 733, lines 26978-26984. That both NICOLESCU and MICLAUS were engaging in separate fraudulent schemes before joining forces, and both made up the core of the group as it evolved and became larger and more sophisticated over ten years, shows a focus and animation that was devoid of self-assessment, remorse, or empathy. In

fashioning a sentence appropriate for such single-minded Defendants, the drumbeat of deterrence must be especially loud and steady.

These defendants have shown no indication that they have disavowed, abandoned, or otherwise disengaged from the beliefs that have led them to this point. NICOLESCU's behavior while incarcerated clearly indicates that he is still more than willing and technically able to apply his technical skills *even behind bars*, and MICLAUS has shown no remorse even after the death of his mother while he was incarcerated and awaiting trial. There has been no evidence to suggest that either would seek legitimate employment upon release. If anything, the opposite is true. With no jobs, no work experience, and an ability to program matched only by their desire to exploit victims, both defendants will only be deterred through denial of access to computers.

In a case of this nature, the only "adequate deterrence to criminal conduct" is complete deterrence, and complete deterrence is accomplished only by a sentence of that keeps both Defendants as far away from victimizing unwitting citizens through stealth, deceit, anonymity, and technical prowess for as long as legally permitted.

C. The Need to Protect the Public

As argued above, these defendants pose a specific and ongoing threat to the public because of their special skills and knowledge, combined with their complete lack or regard or empathy for their victims.[12] What is especially pernicious about these Defendants is that their malware collected data in a manner that can best be described as voracious. The sheer amount of

[12] In Exhibit 1329, a Bayrob member taunts a victim claiming that the loss of money cannot hurt the victim, and somehow they should be thanked for defrauding him. Likewise, in Exhibit 1138, the Bayrob Group demonstrates that their contempt for their victims is unlimited, mocking them with a "Reply to Asshole" button in their eBay Live Chat template. Every potential victim is just an "Asshole" to the Bayrob Group.

data is staggering, but coupled with the efficiency of their ability to cull through and analyze it, the need to protect the public becomes critical.

This harm was graphically documented by the Bayrob Group's practice of taking screenshots of infected computers, and like all important functions of the virus' operation, the Group wrote code to make it automated. *See, e.g.,* Ex. 1137. A review of screenshots found in the Defendants' directories leads to a likely and inevitable parade of horrible exploits. In addition to personal user data relevant to their scheme, screenshots show other personal data such as bank accounts and financial data. *See, e.g.,* Exs. 1175 (Bank of America tab open in the browser) and 1178 (Chase Online tab open in the browser). There are also screenshots reflecting dating sites, and other sites containing personal data which could be used to blackmail the person on whose screen it appears. *See, e.g.,* Ex. 1178. Indeed, this worry is not mere idle speculation. Contained in the ReadNotify collection of emails by the Bayrob Group are emails showing that the Group searched a victim's computer and sent purported evidence of an extra-marital affair to the man's wife. *See* Ex. 1330. This conduct is remorseless, crass, and dangerous.[13] Most disturbing, perhaps, is the screenshot that could have victimized thousands, if not more, individuals across the country. Exhibit 1176 is a schematic for a power plant in Lorain, Ohio. Agents contacted the plant, and learned that, according to experts at the plant, the screen was interactive and if this schematic was followed, it would be possible for a person to hack into the power grid and disrupt power to an entire system. Such a disruption could cost people their lives, cause untold damage to real property, and cause severe disruption to law enforcement and social services.

[13] Additionally, there are other examples of members calling victims vulgar names (*e.g.,* Ex. 1324), and offering rants on the character of their own victims. *See, e.g.,* Ex. 1325.

And on a more personal and individual level, the victim impact statements graphically show the impact on victims. For instance, Ms. Bowes wrote that her life was disrupted, she couldn't eat or sleep and got sick as a result of being defrauded. The Cains were defrauded of $18,000, which they were planning to use for retirement, and felt angry, devastated and foolish; they grew paranoid and suspicious of the internet. Mr. Cole stated that after saving years for a car, he no longer uses eBay and felt distraught and embarrassed. Mr. Kuhlman wrote that even though he recouped some money, he felt stress and lost sleep after being defrauded. Ms. Rohm cried for days and still feels distrustful of anything online, even to the point of questioning the validity of the victim impact statement process. Mr. Wineinger stated that he was defrauded of over $15,000 dollars when he tried to buy a truck for his church to use to help the community. The Boccarossas were defrauded twice when Mr. Boccarossa, a first responder with Engine 205 of the FDNY on 9/11, tried to purchase a car. All 88 victim impact statements reflect similar stories, but are perhaps best represented by the words of Yvonne Moon, who testified at trial and was the first identified victim of the Bayrob Group:

> I testified during this hearing and discussed the financial and emotional hardship this experience caused my family. Those few minutes could never come close to describing the impact this experience has on my life. As a single income home and being a stay at home mom, this literally took our entire savings account. We lost every dollar we had saved and put the remaining balance on a credit card. We already were stretched thin and my husband worked 60 hours a week. We continued to blame one another for what happened which resulted in turmoil within our home. Neither of us was able to move past the experience. I ended up working nights and trying to rebuild the financial state which we were in but our marriage continued to fall apart. We were divorced within a year of this experience. This was one of the hardest years of my life and although I have come a long way since being a victim of this crime, I will always carry the experience with me.
>
> This crime temporarily affected my ability to pay my bills and have a reliable vehicle. This impacted the stability of my marriage and ruined my ability to stay at home and raise my daughters. My entire family

> fell apart because of this experience. If this had not happened to us, it is very possible that my life would be completely different today.

See Victim Impact Statement of Yvonne Moon.

Unfortunately, based on the testimony of former members of the Bayrob Group, reading such victim impact statements will not make NICOLESU or NICOLESCU feel remorse. To the contrary, to Defendants, these statements are simply further evidence of their enormous "power."

Lastly, the harm to the public now, and potentially ongoing in the future, is largely unknown. As discussed in the loss section, the Bayrob Group sold in excess of 10,000 credit cards on Alphabay. Customers of Alphabay are, in no uncertain terms, criminals. Cybercriminals go to sites like Alphabay, and its predecessor Silk Road before it, to buy, sell, and trade stolen identities, credentials and personal information. Vendors sell stolen credentials over and over, and thus, the opportunity to exploit a victim of identity fraud exists as long as that identity is in the possession of a person eager to use it.

Perhaps more disturbing for those victimized by Bayrob was a more recent evolution of their malware in which the malware was instructed to replace a victim's browser with an infected malware version of Mozilla Firefox browser.[14] Once the malicious browser was installed, a user's web traffic was automatically intercepted and compiled by the Bayrob Group. This collection and mining of "big data" is what is on the cutting edge of database and information analytics in Silicon Valley now, and it was the emerging focus of NICOLESCU, DANET, and MICLAUS. Their interest was, however, to geometrically expand their criminal scheme from e-commerce and spam-based exploitation into corporate and financial theft. On the most recent

[14] According to W3Counter, in September 2016 (when Defendants were arrested), FireFox had a 13.1% share of the web browser market, and indeed, the Bayrob Group saved many screenshots of victim computers containing images of Firefox as the browser the victim was using. *See* https://www.w3counter.com/globalstats.php?year=2016&month=9

Command and Control server, SSA Macfarlane found files that allowed the Bayrob Group to search the Firefox web traffic the Bayrob Group ingested for specific terms and cleanly extract the relevant data. For example, in testing this feature, SSA Macfarlane was able to quickly recover over 100 Bank of America user names and passwords, all obtained from Bayrob victims.

As argued above, these Defendants must be kept out of society for as long as possible in order to protect the public. It is not sufficient that NICOLESCU's sister, as stated in the PSR, believes he would never break the law again. Nor is sufficient that both Defendants want to leave the United States upon release. Good wishes and geographic distance are not deterrents to these individuals. To the contrary, Defendants can locate themselves anywhere in the world to commit cybercrimes in the United States. Further, once the Defendants have left the country, it will be very difficult to enforce any requirements of probation or supervised release, and it may not be possible to prevent Defendants from committing even more significant cybercrimes against the United States and its people—this time with the benefit of everything they have learned from discovery and trial in this matter. The only effective deterrent is to remove them from the population for as long as possible.

D. The Need to Provide the Defendant with Rehabilitation Opportunities

The idea that time incarcerated can be transformative and positive in the long run is noble and worthy pursuit. However, everything we know about these Defendants, tells us that such a metamorphosis in this case is chimerical.[15]

NICOLESCU and MICLAUS are both highly intelligent, well-educated, and able to both secure and keep meaningful employment. Growing up in Romania they had the benefit of

[15] As evidenced in their claims of superiority over American victims in Exhibit 1325, no amount of rehabilitation will change the narcissistic but boorishly juvenile high opinion the Defendants have of themselves.

comprehensive educational systems, opportunities for employment, and clear access to technology. Sadly, based on the persistence and length of their scheme, neither defendant has ever taken sufficient steps to veer from a life of crime. Although MICLAUS had occasional legal employment (*e.g.*, as a skydiving instructor), and NICOLESCU had highly marketable skills, neither defendant ever capitalized on those advantages. There is no reason to have any hope that they would do anything but squander resources and opportunities offered to them while incarcerated—resources and opportunities that would be better served and more appreciated going to an inmate sincerely intent on improving his life after release. In the analysis of this purpose for incarceration, great weight should be given to the fact that no amount of assistance would likely benefit the rehabilitation of either defendant. Both are likely to willingly and unrepentantly reoffend at the first opportunity to do so.

E. No Variances Are Warranted After Analyzing the Relevant §3553(a) Factors

It is a "legitimate concern that a lenient sentence for a serious offense threatens to promote disrespect for the law." *Gall*, 128 S.Ct. at 599 (2007); *see also* 18 U.S.C. § 3553(a)(2)(A). Moreover, appropriately reflecting the seriousness of these offenses in turn promotes deterrence and protects the public from further harm from these individuals and others who share their extreme and violent ideology. Taking these factors into account, the Defendants NICOLESCU and MICLAUS should receive terms of 240 months and 216 months imprisonment respectively, as their properly calculated Guidelines suggest and inclusive of their 18 U.S.C. § 1028A convictions.

V. Conclusion

For the foregoing reasons and those presented at the sentencing hearing, the Court should impose a sentence of the should receive terms of 240 months and 216 months imprisonment

respectively for Defendants NICOLESCU and MICLAUS, as their properly calculated Guidelines suggest and inclusive of their 18 U.S.C. § 1028A convictions.

Respectfully submitted,

MICHELLE M. BAEPPLER
First Assistant United States Attorney

By: /s/ Duncan T. Brown
Duncan T. Brown (NY: 3982931)
Brian McDonough (OH: 0072954)
Assistant United States Attorneys
United States Court House
801 West Superior Avenue, Suite 400
Cleveland, OH 44113
(216) 622-3933/3965
(216) 522-8355 (facsimile)
Duncan.Brown@usdoj.gov
Brian.McDonough@usdoj.gov